12/14/95 OPM NO. 5.5.2.1

CRYOGENIC SYSTEM REVIEW

RHIC PROJECT

I. INTRODUCTION

Large quantities of cryogenic fluids are used by the RHIC Project to induce superconductivity in magnets and other test applications. Upon warming, a closed container of cryogenic fluid can become a pressure vessel because the vaporized fluid occupies approximately 700 times the volume of the liquid. As with room temperature pressure vessels, leaks or ruptures can occur with the subsequent release of energy. In addition, cryogenic fluids and materials pose hazards from cold exposure, thermal contraction, brittle fracture and oxygen deficient atmosphere. BNL ES&H Standards 5.1.0 and 5.2.0 pertain to the design and operation of cryogenic systems. Each of these chapters specifies the requirements for dealing with a particular hazard or class of equipment, which may affect the safety of a system.

II. SCOPE

This Standard describes procedures to review and document the safety aspects of cryogenic systems. This Standard also prescribes the required occupational training for cryogenic personnel operating or working near cryogenic systems. It pertains to all cryogenic systems including, for example, those used for refrigerating magnets, or as a source of gas. It also includes cryogenic systems supplying purge gas for detectors where the stored cryogenic liquid inventory is greater than 200 liters.

III. DEFINITIONS

Cryogenic - at a temperature below -150^{o}C.

Cryogenic facility - an area where cryogenic fluids and/or materials are produced, used, or stored.

Cryogenic personnel - those engaged in or responsible for the production, use, transport, or storage of cryogenic fluids and/or materials.

Shall - implies a requirement without deviation.

Should - implies discretion can be used.

Engineered System - a cryogenic system for an experimental device containing a refrigeration source (closed cycle refrigerator or bulk storage) which has been designed with the appropriate safety features.

IV. SPECIAL RESPONSIBILITIES

The Project Head who controls the area of operation of the system is responsible for carrying out the requirements of this Standard. He/she shall:

A. request the Cryogenic Safety Committee (CSC), as early as possible in the design stage, to review each cryogenic system meeting the requirements of Standard 5.1.0 or 5.2.0.

B. provide a safety analysis to the CSC.

C. ensure that the analysis and review are completed prior to operation, preferably prior to construction of the system.

The CSC shall serve the Project in a consulting capacity on all cryogenic system matters.

V. PROCEDURES

Cryogenic systems within the scope of this Standard shall be reviewed. This review shall be completed prior to operation and prior to incorporation of a change in system configuration affecting cryogenic safety. A change in system configuration is not an engine swap or the pumping of a vacuum jacket. System configuration changes are more substantive such as adding a new (including temporary) line, not described in procedures or unusual maintenance operations not previously documented.

A. Safety Analysis and Review

1. The safety analysis shall be performed in accordance with Attachment 1. The analysis and review shall be directed to all aspects of the system which could present a hazard to personnel.

2. The analysis shall demonstrate that the system can be safely brought into operation. It also should demonstrate that safe operation can be maintained.

3. The provisions of ES&H Standards 1.4.1, 5.1.0, 5.2.0 and ASME Codes shall be followed for all cryogenic pressure vessels and pressurized systems capable of a contained pressure of 15 psi or greater.

2. Occupational Training

Occupational and safety training is essential for the safe and efficient operation of cryogenic systems. Training may take the form of safety orientations, safety qualification courses or training by supervisors in accordance with BNL Training Policy. All required training shall be documented.

A. Cryogenic personnel shall have sufficient education, training, and supervision to assure that they can safely perform their duties. Furthermore, personnel shall be instructed in cryogenic hazards specific to the facility at which they work.

B. Until the Supervisor determines that an untrained employee or guest can perform their duties unassisted, he/she shall not work without direct supervision.

Satoshi Ozaki 12/26/95

APPROVED _____ **DATE** _____

RHIC Project Head

CRYOGENIC SAFETY ANALYSIS

Documentation shall be prepared to demonstrate to the CSC that aspects of the system which could present a hazard to equipment or personnel have been examined.

1.0 System Design Documents

1.1 A written system equipment and operation description shall be prepared that will serve as an overview of the system for the CSC and as an introduction for cryogenic facility trainees.

1.2 Complete and accurate P&IDs shall be prepared. The final P&IDs must be signed off as checked and approved.

1.3 An active component list (instrument and valve summary), labeling and describing all active devices of the system shall be prepared. These devices would normally include valves, gages, transducers, brakes, pressure and temperature switches, and rupture disks. In the system, all of these devices shall be identified with permanent tags.

1.4 A list of the system control loops and interlocks and a description of normal operations of each loop or interlock.

2.0 System Operating Documents

2.1 Operations procedures shall be prepared for the system, in accordance with the Project Policy for the Conduct of Operations. All revisions to the operating procedures which could present a hazard to personnel shall be submitted to the CSC.

2.2 Any checklists required for startup, shutdown or normal operation of the system shall be included in the operating procedures.

2.3 The qualification and training requirements of cryogenic personnel, beyond those required in this Standard, shall be defined by the Project and documented.

3.0 Safety Analysis and Documentation

3.1 A System Hazard Analysis shall be performed for all cryogenic engineered systems. The System Hazard Analysis shall be performed to identify hazards associated with component failure modes and functional relationships of components and equipments comprising the system. Such analyses should identify all components and equipment whose performance, performance degradation, functional failure, or inadvertent functioning could result in a hazard. The analysis should include a determination of the modes of failure including all single point failures and the effects on safety when failures occur in system components and equipment. The analysis also shall verify compliance with safety requirements. Techniques that may be used to complete the System Hazard Analysis include Failure Modes and Effects Analysis (Attachment 2), Fault Tree Analysis (Attachment 3), and What-If Analysis (Attachment 4).

3.2 All safety analyses shall be documented. Safety analysis documentation shall address the following elements:

3.2.1 System Description

This section is a summary description of the physical and functional characteristics of the system and its components. Reference to more detailed system and component descriptions, including specifications and detailed review documentation shall be supplied when such documentation is available. The capabilities, limitations and interdependence of these components shall be expressed in terms relevant to personnel and equipment safety. The system and components shall be addressed in relation to its mission and its operational environment. System block diagrams or functional flow diagrams may be used to clarify system descriptions.

3.2.2 Data

This section shall summarize the data used to determine the safety aspects of design features.

3.2.3 Safety Analysis Results

This section shall be a summary or a total listing of the results of safety analyses. Contents and formats may vary according to the individual requirements of the program. The following are the content and format requirements for Safety Analysis Results:

a. A summary of the results.

b. A listing of identified hazards, in narrative of matrix format, to include the following information:

(1) System/Subsystem/Unit. Enter the particular part of the system that this analysis is concerned with. For example; cryogenic pump, to distinguish from a vacuum pump.

(2) Component(s) Failure Mode(s). All component failure modes which can result in a hazard. Failure modes generally answer the question of "how" it fails.

(3) Subsystem Failure Mode(s). The subsystem failure mode descriptions are similar to the component descriptions, however, the emphasis is now placed on failures affecting interfacing subsystem operations

(4) System Component/Phase. The particular phase/component that the analysis is addressing. This could be system, subsystem, component, operating/maintenance procedure or environmental condition.

(5) System Event(s) Phase. The configuration or phase of operation of the system when the hazard could be encountered, such as, maintenance, operation, interlock testing, etc.

(6) System Operation Description. A description of what is normally expected to occur as the result of component/system operation or performance of an operating/maintenance action.

(7) Hazard Description. A brief description of the hazard, such as "Cryogen leak from power lead can." Also, a complete description of the potential/actual hazards inherent in the item being analyzed, or resulting from normal actions or equipment failure.

(8) Hazard Identification/Indication. A description of operator indications which include all means of identifying the hazard to operational and maintenance personnel.

(9) Effect on System. A description of the detrimental effects which could be inflicted upon the system or personnel, resulting from the hazard. Possible upstream and downstream effects also shall be described.

(10) Risk Assessment. A risk assessment for each hazard. This is the classification of hazard severity and probability of occurrence, as defined in ES&H Standard 1.3.3.

(11) Recommended Action. The recommended action required to eliminate or control the hazard. Sufficient technical detail is required in order to permit the design engineers and the customer to adequately develop and assess design criteria resulting from the analysis. Include alternate designs and life cycle cost impact where appropriate.

(12) Effect of Recommended Action. The effect of the recommended action on the assigned risk assessment. Cost/schedule/performance penalties also shall be addressed.

(13) Remarks. Any information relating to the hazard not covered in other blocks.

(14) Status. The status of actions to implement the recommended, or other, hazard controls.

(15) Caution and Warning Notes. A complete list of warnings, cautions, and procedures required in operating and maintenance manuals and for training courses.

3.2.4 Attach FMEA, Fault Tree, and/or "What-If" analyses used to determine the hazards in the system.

4.0 Engineering Documents

4.1 Calculations and/or test results demonstrating the adequacy of the relief system shall be documented.

4.2 Calculations and/or test results shall be prepared to verify that stress levels in materials comply with the requirements of the ASME Code and DOE Order 6430.1A. For designs that are not explicitly covered by the ASME Code, the safety analysis shall show compliance with the intent of the Code and good engineering practice.

4.3 Material certifications, test data, or data sheets shall be obtained and/or documented for any unusual materials used in the system.

4.4 Other calculations required by good engineering practice shall be prepared and documented.

5.0 Maintaining Safe Operation

5.1 Documentation of the system shall be kept current.

5.2 Plans for maintenance and operations shall be prepared and approved before operations begin.

5.3 Operator training and qualification records shall be maintained by the Project.

6.0 Inspections

6.1 Inspections by the CSC may be performed during the review in order to further acquaint the Committee with the system and to clarify safety features of the system.

6.2 Inspections by the CSC may be performed as required during operations to verify continued system safety.

OPM 5.5.2.1 ATTACHMENT 2: 12/14/95

FAILURE MODE AND EFFECTS ANALYSIS

INTRODUCTION

A FMEA requires analysis of the system for all single and probable multiple equipment or operator failures that could cause personnel injury or significant equipment damage. The system shall remain safe for all reasonable postulated equipment failures or operator errors. The analysis is most profitably carried out in parallel with the design effort. A FMEA is best employed as a design tool, not an ad hoc documentation requirement.

PROCEDURE

A FMEA is primarily component oriented. Each component of the system should be reviewed for each possible failed state to determine the effect of the failure on the system and the possible safety consequences to the system. The component list shall include all active components. This includes valves, gauges, transducers, brakes, interlocks, and pressure and temperature switches. A risk assessment is determined for each hazard. This is the classification of hazard severity and probability of occurrence, as defined in ES&H Standard 1.3.3. Decisions shall be made concerning the adequacy of safety. The design shall be approved for safety, and unacceptable risks must be corrected.

DOCUMENTATION

The FMEA should individually list each postulated failure mode for each component. Each failure entry should explain the hazard list or risk assessment, and describe why the mode is failsafe or make a recommendation that will eliminate or mitigate the hazardous condition. See the worksheet at the end of this Attachment.

To be useful, the FMEA must be complete. Every failure of every component must be addressed. Normally this would include only single level failures. Probable multiple failures should also be examined. Other methods can better examine sequential and multiple failure modes (see Fault Tree and What-If, Attachments 3 and 4).

Component_____

Location_____

Date_____

By_____

FAILURE MODE AND EFFECT ANALYSIS

COMPONENT	FAILURE OR ERROR MODE	HAZARD/EFFECT	RISK ASSESSMENT	REMARKS/RECOMMENDATIONS

OPM 5.5.2.1 ATTACHMENT 3: 12/14/95

FAULT TREE ANALYSIS

INTRODUCTION

The purpose of the fault tree analysis is to identify each event and fault which, singly and in all combinations, could cause a specified undesired event. The fault tree analysis is a deductive analytical technique which is qualitative in nature, but can easily be quantified if desired. A fault tree analysis does not model all possible system failures, but only models those faults which can contribute to the specified top event. Hence, proper identification of the top event is essential for complete system hazard identification.

PROCEDURE

The fault tree analysis is a deductive analytical technique. The fault tree results in a graphic and logical representation of the various combinations of possible events, both fault and normal, occurring within a system, which can cause a predefined undesired event. An undesired event is any event which is objectionable or unwanted, such as a potential accident, hazardous condition, or undesirable failure mode. The system is reviewed to determine the conditions, events, and failures that could contribute to the occurrence of the undesired event. These contributing conditions, failures and events are then modeled in a logic tree or diagram, showing their relation to each other and the undesired event being analyzed. The process begins with the immediate necessary and sufficient events that could directly cause the undesirable event (first level). As the procedure goes back step-by-step, combinations of events and failures that could cause the top event. Each part of the system and each condition capable of producing an event is examined for its contribution to the top event and for possible improvement to increase the number of contributions (thereby reducing the probability of occurrence) necessary to cause the event. Suitable mathematical expressions representing the fault tree logic events are developed using Boolean algebra. The resulting mathematical expression of the AND/OR relationships for the tree are then simplified. Probabilities of occurrence are developed for each event in the fault tree and used to compute the probability of occurrence of the top event.

Based upon the information derived from the fault tree evaluation, decisions must be made concerning the adequacy of safety. The design must be approved for safety, and the problem areas must be identified. If the problem areas are identified as unacceptable, corrective action must be taken. Corrective action results in development of preventive measures. Preventative measures are:

- safety design features
- safety devices
- protective systems
- warning devices
- special procedures

As recommended preventative measures are incorporated into the design, their adequacy in solving the safety problem must be verified. This is done by making the appropriate changes to the fault tree logic diagram and re-evaluating the fault tree.

DOCUMENTATION

Documentation of the fault tree consists of the following:

- fault tree logic diagrams
- fault tree probability calculations (for quantitative analysis)
- failure/event rate calculations and/or empirical data used to determine
- probability of occurrence for contributing events
- details of safety improvements
- summary of the final system configuration and the qualitative and quantitative results of the final fault tree analysis.

OPM 5.5.2.1 ATTACHMENT 4: 12/14/95

WHAT-IFS ANALYSIS

INTRODUCTION

This analysis technique examines the consequences of system failures and upsets, as well as procedural errors. This method of analysis examines subsystem rather than components and looks at the effects of external influences on the system. The purpose of this analysis is to reveal any hidden flaws in the design or procedure errors which could present a hazard to personnel and/or equipment.

Procedures using the P&IDs and procedures, "What-if" type questions are asked about each unique mode in the system. These questions are categorized as follows:

a. Each component should be reviewed for unsafe conditions arising from loss of electrical power, loss of instrument air, loss of cooling water, and loss of cryogen, as appropriate.

b. Each system should be reviewed to uncover safety problems arising from contamination in the process stream.

c. Every cold subsystem in the system should be reviewed for safety hazards involving loss of insulating vacuum. Particular attention here should be paid not only to the loss of vacuum, but also damage occurring during a subsequent warmup as cryo-pumped gas evolves, pressurizing the vacuum space.

d. Cryogenic systems should be reviewed to demonstrate that a system will remain safe after refrigeration is lost due to loss of compressors, engines, heat exchangers, vacuum, or power.

e. Each system should be analyzed for the effects of nature (rain, wind, fire, etc.) which have some reasonable chance of occurring.

f. Each system should have its assumptions subjected to the scrutiny of a What-If Analysis; i.e., what if the air system fails.

g. Where the failure of equipment poses a hazard, "What-If" questions should be asked regarding equipment reliability; i.e., what if the drive shaft fails on an expansion engine.

h. Where there is an operator interacting with the system, "What-If" questions should be asked. (In general, if the FMEA has been completed, the operator should be able to position any single element (valve) without a hazard.)

I. Each subsystem should be examined for likely multiple failure. (This section may be done in the format of a system Hazards Analysis in Attachment 1.)

PROCEDURES

1. Work with P&IDs and system procedures (operating, repair, etc.).

2. Go through each step of the procedure and examine the consequence of each action specified.

3. Questions of multiple failures may also be asked (i.e., what if step n of a procedure is initiated and there is a failure of device m?) These questions should be restricted to probable failures.

4. Evaluate the consequences of each "What-If" situation.

5. Determine the risk assessment for each hazard. This is the classification of hazard severity and probability of occurrence, as defined in ES&H Standard 1.3.3.

6. Decisions shall be made concerning the adequacy of safety. The design shall be approved for safety, or unacceptable risks must be corrected.

DOCUMENTATION

All "What-If" situations analyzed shall be documented using a "What-If" worksheet. Each description shall completely and unambiguously describe each element. Design changes shall be noted by drawing and/or change number. Procedural changes shall be defined by step number.

Component_____

Location_____

Date_____

By_____

WHAT-IF WORKSHEET

WHAT-IF	CONSEQUENCE/HAZARD	RISK ASSESSMENT	CONCLUSION/RECOMMENDATIONS